Hybrid Warfare and Cognitive Defense

The Weaponization of Human Neuroplasticity in Modern Conflict

Manuel Pereira & Claude Sonnet 4.5

October 2025

Abstract

This paper examines the evolution of hybrid warfare beyond traditional cyberattacks and infrastructure disruption to its most insidious dimension: cognitive warfare targeting human neuroplasticity. As NATO Allied Command Transformation recognizes, cognitive warfare represents a paradigm shift where "the human mind becomes the battlefield"[1]. This analysis argues that children represent the primary strategic target in cognitive warfare operations, as their developing brains are uniquely vulnerable to AI-powered psychological operations operating at unprecedented scale and sophistication. The paper demonstrates why traditional "peace by war" doctrine fails against adversaries employing cognitive warfare tactics, explores the attribution problem in AI-planned attacks, and proposes educational frameworks for building cognitive resilience as critical national defense infrastructure. Drawing on recent research in neurodevelopment, AI-generated disinformation, and military strategic doctrine, this work contends that we are currently losing a generational war for cognitive sovereignty, with implications extending far beyond traditional security concerns to the foundational stability of democratic societies.

[1]NATO Allied Command Transformation. (2021). Countering cognitive warfare: awareness and resilience. *NATO Review*. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

Contents

1. Introduction: From "Peace by War" to Cognitive Warfare

The traditional concept of "peace by war" suggests that lasting peace can be achieved through decisive military conflict. This philosophy, embodied in the Roman maxim *si vis pacem, para bellum* (if you want peace, prepare for war), rests on assumptions of identifiable adversaries, geographic battlefields, and clear victory conditions. However, modern hybrid warfare operates in a fundamentally different paradigm that challenges these foundational assumptions.

NATO defines hybrid warfare as the integration of cyber, information, psychological, and social engineering capabilities that operate below the traditional threshold of armed conflict[2]. Within this framework, cognitive warfare has emerged as perhaps the most significant evolution. As NATO Allied Command Transformation articulates, "In cognitive warfare, the human mind becomes the battlefield. The aim is to change not only what people think, but how they think and act."

This represents more than sophisticated propaganda. Cognitive warfare weaponizes human neuroplasticity itself—the brain's fundamental capacity to reorganize and form new neural connections throughout life. What evolution designed as an adaptive mechanism for learning and survival becomes, in the context of modern information warfare, a strategic vulnerability that can be systematically exploited.

2. The Attribution Problem in Hybrid Warfare

Traditional "peace by war" doctrine requires identifying who to fight. Hybrid warfare, particularly AI-planned cyberattacks, introduces profound attribution challenges that undermine conventional military responses. Attacks can be routed through compromised systems in neutral countries, executed by non-state actors with ambiguous state sponsorship, designed with plausible deniability built into their architecture, and automated to the point where even the initiating actor has limited ongoing control.

2.1. Current Military Adaptations

NATO has developed what it terms "integrated deterrence" as a response to these challenges, incorporating cyber-on-cyber responses, economic warfare through sanctions, information operations for counter-propaganda, and conventional military backup for certain escalation thresholds. The United States has adopted a "defend forward" strategy involving persistent engagement in adversary networks, operating preemptively rather than reactively.

However, these adaptations face a fundamental conceptual problem: hybrid warfare offers no clear endpoint. There is no surrender ceremony for bot networks, no territorial capture to mark victory, no definitive moment when cognitive operations cease. The traditional military concept of forcing peace through decisive victory may simply not apply to this form of perpetual, low-intensity conflict.

2.2. The AI Complication

AI-planned attacks compound attribution difficulties through speed of execution that outpaces human response capabilities, sophisticated attack vectors that evolve faster than defensive measures, effective obscuring of operational origins, and emergent behaviors that create unin-

[2]NATO. (2021). Hybrid warfare – new threats, complexity, and 'trust' as the antidote. *NATO Review*. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

tended escalation dynamics[3]. This creates scenarios where neither attacker nor defender fully controls the conflict trajectory, fundamentally undermining traditional deterrence theory.

3. The Brain as Critical Infrastructure

Traditional warfare targets physical infrastructure: bridges, power plants, communication networks, supply lines. Hybrid warfare targets something more foundational: consensus reality —the shared understanding of what is true that enables societies to function collectively. The human brain's plasticity, normally an evolutionary advantage enabling learning and adaptation, becomes a vulnerability when systematically exploited.

3.1. Understanding the Neurological Vulnerability

Several well-documented cognitive mechanisms create exploitable vulnerabilities in information warfare:

- **Illusory truth effect:** The brain treats familiar information as more trustworthy, regardless of veracity. Repeated exposure to false claims increases perceived credibility.
- **Emotional prioritization:** Neural architecture privileges emotionally charged information over analytical processing, making emotion-laden disinformation more impactful than fact-based corrections.
- **Social proof mechanisms:** Humans are neurologically wired to align with perceived group consensus, making manufactured consensus particularly effective.
- **Confirmation bias:** The tendency to seek, interpret, and recall information confirming preexisting beliefs creates predictable exploitation patterns.

4. AI-Generated Propaganda: A Qualitative Leap

Previous propaganda efforts were constrained by human capacity to produce and distribute content. Artificial intelligence fundamentally transforms the operational landscape of information warfare, creating capabilities that represent a qualitative rather than merely quantitative shift.

4.1. Scale and Personalization

AI systems can generate millions of unique persuasive messages, each tailored to individual psychological profiles derived from behavioral data. Rather than broadcast messaging, contemporary cognitive warfare creates individualized "reality tunnels"—each target receives content calibrated to their specific vulnerabilities, fears, desires, and cognitive biases. Research indicates that deepfake technology increased by 118% in 2024 alone, with 90% of U.S. companies experiencing some form of AI-enhanced cyber fraud[4].

4.2. Persistence and Adaptive Learning

Automated systems maintain continuous presence, gradually shifting perceptions through sustained, low-intensity exposure rather than obvious persuasion attempts. These systems learn in real-time what approaches prove effective, continuously optimizing for engagement and belief modification. The sophistication of AI-generated deepfakes and synthetic media makes distin-

[3]Claverie, B., & du Cluzel, F. (2023). The cognitive warfare concept. NATO Innovation Hub. https://innovationhub-act.org/

[4]European Parliamentary Research Service. (2025). AI-based deepfakes and disinformation. European Parliament Briefing. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf

guishing authentic from fabricated content increasingly impossible without technical verification most populations cannot perform[5].

4.3. The Fake News Ecosystem as Weapon System

In hybrid warfare context, disinformation operates as cognitive infrastructure attack designed to:

1. Erode trust in institutions, making populations unable to distinguish authoritative information from noise
2. Create manufactured divisions that prevent societal unity against external threats
3. Normalize previously unthinkable positions by gradually shifting acceptable discourse boundaries
4. Induce learned helplessness by overwhelming people with contradictory information until they cease attempting to discern truth
5. Hijack attention with manufactured controversies while strategic moves proceed unnoticed

The critical characteristic of this approach: victims remain unaware they are under attack, believing instead they are forming independent opinions through their own research and critical thinking[6].

5. Children: The Strategic Long Game

Figure 1: In a hybrid, long- standindg war, children are a vulnerable and valuable target.

Children represent the most vulnerable and strategically valuable targets in cognitive warfare.

This is not hyperbole but recognition of neurodevelopmental realities and strategic timescales fundamentally different from traditional military operations.

5.1. Neurological Vulnerability

Research demonstrates that developing brains exhibit heightened neuroplasticity, making early exposure to manipulated information formative rather than merely influential. A longitudinal study published in *JAMA Pediatrics* found that adolescents who habitually check social media show significant changes in brain regions controlling social rewards and punishment, particularly in the development of the brain's reward circuitry[7].

[5]U.S. Government Accountability Office. (2024). Science & tech spotlight: combating deepfakes. GAO Report GAO-24-107292. https://www.gao.gov/products/gao-24-107292

[6]Department of Homeland Security. Increasing threats of deepfake identities. DHS Publications. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

[7]Maza, M. T., et al. (2023). Association of habitual checking behaviors on social media with longitudinal functional brain development. *JAMA Pediatrics*. University of North Carolina

Current generations spend formative developmental years in algorithmically curated environments. The U.S. Surgeon General's 2023 advisory on social media and youth mental health reports that up to 95% of youth ages 13-17 use social media platforms, with nearly 40% of children ages 8-12 also active users[8]. Critically, one-third of teenagers report using social media "almost constantly," meaning their cognitive development occurs within information environments optimized for engagement rather than truth or wellbeing.

5.2. Long-Term Strategic Value

Cognitive warfare targeting children operates on generational timescales fundamentally different from traditional military operations. A child influenced at age 8 becomes a voter, worker, policymaker, and parent at age 28—with two decades of embedded narratives shaping decision-making, institutional trust, and worldview formation. This represents strategic depth unavailable through conventional military operations.

5.3. The Toxic Content Pipeline

Children currently experience exposure to conspiracy theories packaged as "questioning authority," extremist content embedded in gaming communities and meme culture, commercial manipulation equating consumption with identity formation, algorithmic radicalization where each interaction leads deeper into ideological rabbit holes, and synthetic social comparison generating documented increases in anxiety, depression, and body dysmorphia. Research shows strong correlations between frequent social media use and lower self-esteem, depressive symptoms, anxiety, and other mental health challenges in children[9].

6. Education as Cognitive Immunity

If the human brain constitutes critical infrastructure in hybrid warfare, education becomes national defense. However, traditional "media literacy" proves insufficient against AI-powered psychological operations. Comprehensive cognitive defense requires more sophisticated approaches.

6.1. Critical Thinking as Immune System Development

Effective cognitive defense education must address several dimensions:

6.1.1. Epistemology Education

Teaching children how we know what we know: distinguishing evidence from assertion, tracing information to primary sources, understanding differences between expert consensus and opinion, and recognizing logical fallacies and emotional manipulation techniques.

6.1.2. Metacognition Training

Developing capacity to observe one's own thinking processes: questioning why content generates particular emotional responses, identifying intended belief or behavioral changes, considering alternative perspectives, and recognizing how personal biases influence interpretation.

---

at Chapel Hill. https://www.unc.edu/posts/2023/01/03/study-shows-habitual-checking-of-social-media-may-impact-young-adolescents-brain-development/

[8]U.S. Surgeon General. (2023). Social media and youth mental health: The U.S. Surgeon General's advisory. U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf

[9]Al-Harbi, M., et al. (2024). The impact of social media on children's mental health: a systematic scoping review. *Cureus*, 16(11). https://pmc.ncbi.nlm.nih.gov/articles/PMC11641642/

6.1.3. Digital Forensics Basics

Providing age-appropriate technical skills: reverse image searching, source credibility verification, synthetic media artifact recognition, and understanding algorithmic content curation mechanisms.

6.1.4. Emotional Regulation

Since propaganda systematically exploits emotional responses: teaching children to pause before reacting, recognizing content designed to trigger outrage, developing resilience to social pressure, and understanding manipulation of fear and anger responses.

6.2. Experiential Inoculation

Like medical vaccines exposing immune systems to weakened pathogens, cognitive inoculation exposes children to "weakened" manipulation attempts in controlled environments. This includes:

- Analyzing how persuasive techniques function in advertising before recognizing identical techniques in political content
- Having children themselves create propaganda to understand mechanics
- Gamifying "spot the manipulation" exercises to make detection instinctive
- Examining historical propaganda case studies from ancient Rome through modern periods to demonstrate recurring patterns

6.3. Building Cognitive Resilience

Long-term resilience requires exposing children to diverse information sources representing multiple perspectives on controversial issues, direct primary sources rather than commentary, content challenging emerging worldviews, and international perspectives revealing cultural assumptions. Additionally, teaching collaborative truth-seeking—how scientific peer review functions, why communities of practice develop specialized expertise, and distinguishing genuine debate from manufactured controversy—helps children understand knowledge as socially constructed rather than individually determined.

6.3.1. Identity Beyond Consumption

Helping children develop self-worth not based on likes, follows, or views; interests that exist offline; face-to-face community connections; and skills and accomplishments independent of digital validation.

7. The Current Reality: Already Inside the War

The uncomfortable truth: we are not preparing for cognitive warfare; we are currently losing it. Children today inhabit hostile cognitive environments where algorithms optimize for engagement—which neuroscience demonstrates means outrage, fear, and tribalism—during critical developmental windows[10]. Many unknowingly participate in information warfare by sharing manipulated content, becoming nodes in propaganda distribution networks.

7.1. The Strategic Logic of Cognitive Warfare

Traditional warfare pursues geographic objectives: territorial capture, capability destruction, forced surrender. Hybrid warfare pursues psychological objectives: making adversaries defeat

[10]Yale Medicine. (2024). How social media affects your teen's mental health: a parent's guide. Yale Medicine News. https://www.yalemedicine.org/news/social-media-teen-mental-health-a-parents-guide

themselves. Research on hybrid threats emphasizes that the information, cognitive, and social domains have become the cornerstone of modern hybrid warfare operations.

Why engage in costly kinetic conflict when cognitive operations can: undermine trust in adversary institutions, turn citizens against each other, paralyze decision-making through information overload, make populations voluntarily adopt positions serving hostile interests, and raise generations questioning their own system's legitimacy?

7.2. The Attack Surface and Time Horizon

In hybrid warfare, every connected device represents a potential entry point, but the target is not the device—it is the mind using it. Cyberattacks on infrastructure cause temporary disruption; cognitive attacks on populations cause permanent transformation. Traditional military campaigns operate on timescales of months to years. Cognitive warfare operates on generational timescales: shaping basic worldview, trust patterns, and information processing habits in years 0-10; reinforcing through adolescent identity formation in years 10-20; and harvesting a generation with embedded assumptions favorable to adversary interests from age 20 onward.

This temporal dimension suggests that children's exposure to toxic content is not a side effect of hybrid warfare—it may constitute the primary battlefield.

7.3. The Defense Dilemma

Traditional defense proves conceptually simpler: walls, weapons, training. Cognitive defense requires free societies to restrict information (an authoritarian solution defeating its own purpose), technology companies to prioritize truth over profit (unlikely without comprehensive regulation), educational systems to adapt faster than historical precedent, parents to enforce boundaries against sophisticated addiction mechanisms, and international cooperation against adversaries actively employing these techniques.

We face the challenge of defending open societies against closed-society tactics specifically engineered to exploit openness as vulnerability. As NATO research acknowledges, this creates fundamental tensions between security and democratic values.

7.4. Integrating Into Hybrid Warfare Framework

This cognitive dimension isn't separate from hybrid warfare—it's the keystone. Every connected device is a potential entry point, but the target isn't the device—it's the mind using it. You can rebuild a power grid; rebuilding shared consensus reality proves far more difficult.

8. Conclusion

In traditional warfare, victory involves enemy surrender and territorial occupation. In cognitive hybrid warfare, no clear victory conditions exist—only degrees of resilience measured by population capacity to distinguish true from false, citizen trust enabling collective action, resistance to emotional manipulation, maintenance of functional disagreement without societal fracture, and successive generations' vulnerability levels.

Without intervention, current trajectories lead toward societal immune deficiency where populations lack resistance to information manipulation; permanent epistemic crisis eliminating shared basis for determining truth, making governance progressively impossible; generational capture with cohorts raised entirely within algorithmically curated realities shaped by hostile actors and amoral profit-maximizing systems; and democratic collapse occurring not through

coup or invasion but through populations unable to agree on basic facts necessary for democratic function.

If we accept that the human mind constitutes critical infrastructure in hybrid warfare, education becomes national defense. This requires digital literacy programs receiving defense-level priority, protecting children's cognitive development as aggressively as physical infrastructure, treating algorithmic manipulation of minors as national security threats, and investing in cognitive resilience with the same urgency applied to cybersecurity.

The paradox remains: societies most vulnerable to cognitive warfare (open democracies) are least equipped to defend against it without compromising the openness making them valuable. Yet the alternative—allowing generational cognitive conscription by adversaries or amoral algorithms—constitutes civilizational surrender.

The real hybrid war is not fought with drones and malware. It is being fought inside the minds of children engaging with screens at this moment, their neuroplasticity weaponized against them while societies debate whether screen time is "really that bad." The question is not whether education can vaccinate children against false realities. The question is whether we will recognize the urgency before losing a generation—and through them, the war.

8.1. A Reconceptualized Framework

A reconceptualized framework for modern security must include:

"Stability through persistent competition": Accepting ongoing conflict as the norm and focusing on maintaining acceptable equilibrium rather than decisive victory.

"Resilience as defense": Making societies immune or highly resistant to threats that cannot be eliminated.

"Cost imposition": Making hybrid aggression expensive enough through comprehensive means that adversaries choose not to escalate.

"Norms and consequences": Building international consensus on unacceptable behavior with collective response mechanisms.

We may be entering an era of permanent low-intensity conflict where "peace" means "manageable levels of hostility" rather than absence of aggression. This requires fundamental rethinking of security extending beyond military doctrine into diplomacy, economics, technology policy, education, and social cohesion. The "enemy" in hybrid warfare might be less a specific adversary and more a condition of perpetual competition requiring management rather than victory.

9. References

NATO Allied Command Transformation. (2021). Countering cognitive warfare: awareness and resilience. *NATO Review*. https://www.nato.int/docu/review/articles/2021/05/20/countering-cognitive-warfare-awareness-and-resilience/index.html

NATO. (2021). Hybrid warfare – new threats, complexity, and 'trust' as the antidote. *NATO Review*. https://www.nato.int/docu/review/articles/2021/11/30/hybrid-warfare-new-threats-complexity-and-trust-as-the-antidote/index.html

Claverie, B., & du Cluzel, F. (2023). The cognitive warfare concept. NATO Innovation Hub. https://innovationhub-act.org/

European Parliamentary Research Service. (2025). AI-based deepfakes and disinformation. European Parliament Briefing. https://www.europarl.europa.eu/RegData/etudes/BRIE/2025/775855/EPRS_BRI(2025)775855_EN.pdf

U.S. Government Accountability Office. (2024). Science & tech spotlight: combating deepfakes. GAO Report GAO-24-107292. https://www.gao.gov/products/gao-24-107292

Department of Homeland Security. Increasing threats of deepfake identities. DHS Publications. https://www.dhs.gov/sites/default/files/publications/increasing_threats_of_deepfake_identities_0.pdf

Telzer, E. H., et al. (2022). Longitudinal associations between social media use, mental well-being and structural brain development across adolescence. *Developmental Cognitive Neuroscience*, 54, 101088.

Maza, M. T., et al. (2023). Association of habitual checking behaviors on social media with longitudinal functional brain development. *JAMA Pediatrics*. University of North Carolina at Chapel Hill. https://www.unc.edu/posts/2023/01/03/study-shows-habitual-checking-of-social-media-may-impact-young-adolescents-brain-development/

U.S. Surgeon General. (2023). Social media and youth mental health: The U.S. Surgeon General's advisory. U.S. Department of Health and Human Services. https://www.hhs.gov/sites/default/files/sg-youth-mental-health-social-media-advisory.pdf

Al-Harbi, M., et al. (2024). The impact of social media on children's mental health: a systematic scoping review. *Cureus*, 16(11). https://pmc.ncbi.nlm.nih.gov/articles/PMC11641642/

Yale Medicine. (2024). How social media affects your teen's mental health: a parent's guide. Yale Medicine News. https://www.yalemedicine.org/news/social-media-teen-mental-health-a-parents-guide